

## UNITED STATES DISTRICT COURT

for the  
Eastern District of MichiganIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)A silver iPhone 12 Pro Max  
(More fully described in Attachment A)

Case No. 2:21-mc-51096 -1

Judge: Steeh, George Caram

Filed: 08-20-2021

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See ATTACHMENT A.

located in the Eastern District of Michigan, there is now concealed (identify the person or describe the property to be seized):

See ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

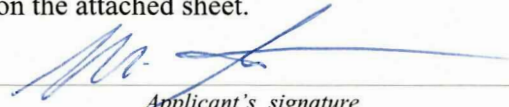
18 U.S.C. 1591

Sex trafficking of children or by force, fraud, or coercion

The application is based on these facts:

See attached AFFIDAVIT.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Michael Strunk, Task Force Officer (FBI)

Printed name and title

Sworn to before me and signed in my presence  
and/or by reliable electronic means.

Date: August 20, 2021

City and state: Bay City, Michigan



Judge's signature

Hon. Patricia T. Morris U. S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Michael Strunk, Task Force Officer with the Federal Bureau of Investigation (FBI), swear and affirm as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been employed by the Detroit Police Department for six years and have been a Task Force Officer for approximately three years with the FBI, as I currently work on the Southeast Michigan Trafficking and Exploitation Crimes (SEMTEC) Task Force. I have experience investigating child sexual exploitation and human trafficking crimes and have also been trained specifically on these types of investigations. I have consulted with numerous other SEMTEC agents, including those that have worked on human trafficking investigations for many years.

3. This affidavit is based on information I personally obtained, as well as information I received from law enforcement officers and agents who participated

in this investigation. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

**IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

4. The property to be searched is: (1) silver Apple iPhone 12 Pro Max (the SUBJECT DEVICE). The SUBJECT DEVICE is located at the FBI's Detroit Field Office Evidence Control Room, 477 Michigan Ave, Detroit, MI 48226.

5. The applied-for warrant would authorize the forensic examination of the SUBJECT DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

**JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

**PROBABLE CAUSE**

**A. Investigation of DAVIS**

7. On December 10, 2020, Ingham County Department of Health and Human Services Child Protective Services (CPS) investigator, Gena Jorgensen (Jorgensen), contacted the Federal Bureau of Investigation (FBI), Lansing Resident Agency to report two sixteen year-old juveniles actively being sex trafficked in the Detroit area, hereinafter MINOR 1 and MINOR 2. Jorgensen confirmed both MINOR 1 and MINOR 2 were active runaways from Lansing, Michigan.

8. Jorgensen was assigned to investigate and locate MINOR 1 and MINOR 2. On December 10, 2020, Jorgensen received a call from the grandmother and custodian of MINOR 1 reporting new information on MINOR 1's whereabouts. The grandmother reported that MINOR 1 reached out several times over a three-day period to MINOR 1's aunt and MINOR 1's biological mother. MINOR 1 initially said she was with MINOR 2 in Indiana selling marijuana and would be back in a couple of days. Later, an individual contacted MINOR 1's biological mother, using telephone number XXX-XXX-0873. The individual stated MINOR 1 left with a pimp who dropped her off with an unknown person.

9. After being contacted by XXX-XXX-0873, MINOR 1's mother researched the phone number on the internet and located an escort ad that included

phone number XXX-XXX-0873. MINOR 1's mother provided the advertisement to law enforcement. When law enforcement viewed the advertisement, they saw that it was an advertisement for commercial sexual purposes. The ad listed the contact number XXX-XXX-0873 and contact name "Mimi." Images associated with the advertisement depicted young females in sexually explicit positions, including underwear, lingerie, and exposed genitals. Three of the pictures depicted MINOR 1, and two pictures depicted MINOR 2. A female, later identified as MINOR 3 was also depicted in the advertisements.

10. On December 10, 2020, the FBI located additional Internet posts advertising MINOR 1 and MINOR 2 for commercial sex in the Detroit area. The advertisements included XXX-XXX-0873 as a means to schedule a commercial sex date.

11. On December 10, 2020, a law enforcement officer (in an undercover capacity) contacted XXX-XXX-0873 and arranged a commercial sex date. The person who answered the phone (XXX-XXX-0873) provided the officer with instructions on where and how to meet. The officer was directed to the Hawthorne Suites in Detroit. Once at the hotel, the officer was directed to Room 613 where he met MINOR 3. Other officers and agents arrived on the scene and recovered MINOR 3 who is 16 years old and from the Lansing area.

12. Law enforcement determined, using a public database, that phone number XXX-XXX-0873 was assigned to Bandwidth, a communications platform.<sup>1</sup> Law enforcement contacted Bandwidth seeking information about phone number XXX-XXX-0873, and Bandwidth responded that XXX-XXX-0873 was assigned to TextNow.

13. Law enforcement then requested subscriber information from TextNow. TextNow responded that the user of XXX-XXX-0873 had provided an email address associated with MINOR 3.<sup>2</sup>

14. On December 10, 2020 and December 22, 2020, MINOR 3 spoke with law enforcement and permitted the review of her cell phone. In MINOR 3's phone, agents saw contact information for MINOR 1 and MINOR 2.

15. During her interviews with law enforcement on December 10 and December 22, 2020, MINOR 3 stated:

- a. She ran away from her mother's home eight months ago and has been supporting herself since she left by engaging in commercial sex dates.

---

<sup>1</sup> Bandwidth is a communications platform. Bandwidth sells software application programming interfaces for voice and messaging, using their own IP voice network.

<sup>2</sup> The email address included MINOR 3's first and last name.

She stated she was not working for any pimps and kept all the proceeds from her dates for herself.

- b. She had previously called MINOR 1's mother to try and find out where MINOR 1 was.
- c. She knew MINOR 1 and MINOR 2 and that they had previously been with her in the Detroit area.
- d. She assisted MINOR 1 and MINOR 2 with engaging in commercial sex by posting ads for them online and communicating with men on their behalf. She posted ads using a TextNow number and communicated with clients using a TextNow number.
- e. She ran away from her home approximately eight months prior. She engaged in commercial sex acts and lived out of hotels in the metro Detroit area.
- f. She denied working for anyone and said that she kept all the proceeds from commercial sex dates. She further stated that she paid her friend "Fazo" to rent hotel rooms for her since MINOR 3 is underage.

16. The FBI obtained a copy of the Hawthorne Suites folio for Room 613. The folio showed that on December 7, 2020, Room 613 was rented by TORIANO

DAVIS (DOB: XX/XX/1988) who provided a North Dakota driver's license. The driver's license showed that DAVIS was born in 1988.

17. On December 11, 2020, a magistrate judge in the Western District of Michigan issued a federal search warrant for GPS location pings for the cellular phones of MINOR 1 and MINOR 2. GPS pings showed the location of one of the phones in the vicinity of the Red Roof Inn, 27660 Northwestern Highway, Southfield, MI. On December 11, 2020, law enforcement responded to the Red Roof Inn in Southfield, and located MINOR 1 and MINOR 2 in Room #129.

18. On December 11, 2020, and January 7, 2021 MINOR 1 spoke with law enforcement. During her interviews, MINOR 1 stated:

- She was planning on running away with MINOR 2. She contacted MINOR 3 for a ride, and MINOR 3 sent an adult male to pick-up MINOR 1;
- An adult male picked MINOR 1 up from the Lansing, Michigan area and transported her to a hotel in the Detroit, Michigan area. MINOR 1 said that MINOR 3 then paid for the transportation;
- After arriving in the Detroit area, MINOR 1, MINOR 2, and MINOR 3 spent time in multiple hotel rooms in the area;
- MINOR 3 posted ads for commercial sex using images of MINOR 1 and MINOR 2;



- MINOR 3 arranged the meetings for commercial sex, with MINOR 1 and MINOR 2, primarily through text message and phone calls;
- MINOR 3 took the money from the dates for commercial sex with MINOR 1 and MINOR 2;
- After collecting payment, MINOR 3 provided the money to TORIANO DAVIS;
- MINOR 1 believed MINOR 3 collected \$700 for the dates MINOR 3 arranged for MINOR 1;
- MINOR 1 was only paid \$20 out of the \$700. MINOR 1 believed she owed a debt to MINOR 3 and DAVIS for transportation and hotel rooms;
- MINOR 1 stated MINOR 3 was acting as a “trainer” to MINOR 1 and MINOR 2 showing them how the commercial sex trade works;
- MINOR 3 had a TextNow number that she used to set up the commercial sex dates and communicate with customers;

19. On December 11, 2020, and January 27, 2021, MINOR 2 spoke with law enforcement. During her interviews, MINOR 2 provided many of the same facts provided by MINOR 1. MINOR 2 also stated:

- MINOR 1 and MINOR 2 took pictures of each other in lingerie and provided the images to MINOR 3 to be added to the escort ad;

- “Tori” (believed to be TORIANO DAVIS) took sexually explicit pictures of MINOR 3 with her cell phone for the escort advertisements;
- DAVIS and MINOR 3 picked up MINOR 1 and MINOR 2 and conveyed them to a hotel in Detroit, Michigan, where DAVIS purchased rooms for the girls to perform sex dates;
- MINOR 3 collected the money made from commercial sex and provided it to “Tori”;
- MINOR 3 added the photographs that MINOR 1 and MINOR 2 sent her to an escort ads;
- MINOR 3 communicated with whomever responded to the ads;
- MINOR 2 performed (4) four commercial sex dates;
- MINOR 3 would greet the john and introduce MINOR 2, take the money and leave the room;
- MINOR 3 would come back to the room and give MINOR 2 \$20-\$60 for performing the service;
- MINOR 3 would give DAVIS all of the money made from the dates;
- MINOR 3 intimidated MINOR 1 and MINOR 2 on multiple occasions by threatening and yelling at them.

20. On August 3, 2021, SEMTEC received several tips that MINOR 3 was with her suspected trafficker DAVIS. Through known telephone numbers and facial recognition, SEMTEC discovered multiple commercial sex ads depicting pictures of MINOR 3. Several attempts were made by an undercover officer to set up a sex date with MINOR 3, and the undercover was given an address by MINOR 3 to meet. Then MINOR 3 stopped all communication.

21. On August 3, 2021 SEMTEC received information that DAVIS was staying at the Quality Inn Hotel, 31960 Little Mack, Roseville, MI. SEMTEC members went to the front desk of the hotel and told hotel staff that DAVIS was believed to be staying in the hotel and was known to be trafficking minors. The hotel staff confirmed DAVIS was at the hotel in Room 125, and stated that they planned to evict DAVIS based on the information that SEMTEC provided.

22. Hotel staff proceeded to Room 125 with SEMTEC members accompanying them. Hotel staff knocked on the door, and DAVIS opened the door completely nude. Hotel staff evicted DAVIS from the room. A completely nude unknown female was also discovered in the bed in Room 125. Law enforcement entered Room 125 to identify and speak with the unknown female. Based on information known to SEMTEC at the time, law enforcement believed

that the unknown female in DAVIS's room was MINOR 3. The unknown female was later identified as MINOR 4, a 15 year-old female.

23. In Room 125, law enforcement observed used condom wrappers throughout the room. Law enforcement also observed two cellular phones. I observed the SUBJECT DEVICE on the bed in Room 125, and DAVIS claimed it as his cellular phone. MINOR 4 claimed the other cellular phone. SEMTEC recovered the phones, and they are currently located at the FBI's Detroit Field Office Evidence Control Room, 477 Michigan Ave., Detroit, MI 48226.

24. On August 3, 2021, MINOR 3 spoke with law enforcement. During her interview, MINOR 3 stated:

- DAVIS took earnings from the dates for personal use, including purchasing marijuana and controlled substances, such as ecstasy;
- DAVIS would supply ecstasy to MINOR 4 on a regular basis;
- MINOR 3 would conduct commercial sex dates during her stay with DAVIS to buy him whatever he wants;
- MINOR 3 conducted dates with DAVIS and MINOR 4;
- MINOR 4 reached out to MINOR 3 for a place to stay after admitting she had been walking the "track." MINOR 3 explained the dangers in doing that and taught MINOR 4 how to set up ads.

25. On August 5, 2021 MINOR 3 escaped from the custody of Michigan Department of Health and Human Services. MINOR 3 has not yet returned and has not yet been located.

26. On August 8, 2021, MINOR 4 signed a consent to search form to conduct a forensic analysis of her phone. The examination of the phone revealed messages between MINOR 4 and an individual believed to be DAVIS, who is referred to in the phone “T.” The content of those messages are as follows:

<b>Date/Time</b>	<b>Author (Sender)</b>	<b>Message</b>
7/23/2021 2:49:17 AM	T XXX-XXX-8149	You ready to work
7/23/2021 2:49:27 AM	MINOR 4 XXX-XXX-0341	Yes
7/23/2021 2:49:41 AM	T XXX-XXXX-8149	Ok I'll repost
7/23/2021 2:49:50 AM	MINOR 4 XXX-XXX-0341	okay
7/23/2021 2:49:53 AM	T XXX-XXX-8149	Are you hungry do you want to eat first

7/24/2021 5:02:55 AM	T XXX-XXX-8149	Bae try and get it in
7/24/2021 5:03:01 AM	MINOR 4 XXX-XXX-0341	ok
7/24/2021 5:30:15 AM	MINOR 4 XXX-XXX-0341	Lmk when you see him
7/24/2021 5:30:19 AM	T XXX-XXX-8149	ok
7/24/2021 5:30:55 AM	T XXX-XXX-8149	He coming
7/24/2021 6:26:54 AM	MINOR 4 XXX-XXX-0341	Ok Tori I don't feel like arguing bc u wanna start sum for no reason
7/24/2021 6:27:16 AM	T XXX-XXX-8149	You the one acting like you have an attitude
7/24/2021 6:27:26 AM	MINOR 4 XXX-XXX-0341	No I'm not

7/24/2021 6:27:38 AM	T XXX-XXX-8149	ok
7/24/2021 6:28:13 AM	MINOR 4 XXX-XXX-0341	I don't like doing this shit and all I hear outta your mouth is how I need to keep doing it.
7/24/2021 6:28:57 AM	MINOR 4 XXX-XXX-0341	Like wtf do I even get out of doing this? Nothing, u get way more out of it than I do and I tired
7/24/2021 6:28:57 AM	T XXX-XXX-8149	Say less
7/24/2021 6:29:13 AM	MINOR 4 XXX-XXX-0341	I barely ask you for anything and when I do I hardly ever get it
7/24/2021 6:30:04 AM	MINOR 4 XXX-XXX-0341	Like wow I asked to get my nails done, can't even do that. But when you wanna drive these cars and stay in nice rooms you get that
7/24/2021 6:30:24 AM	MINOR 4 XXX-XXX-0341	Even [MINOR 3] is getting more than me

7/24/2021 6:30:34 AM	T XXX-XXX-8149	I'm done it's ok over fuck it never again
7/24/2021 6:30:54 AM	MINOR 4 XXX-XXX-0341	Excuse me?
7/24/2021 6:32:31 AM	MINOR 4 XXX-XXX-0341	I'm not saying I won't do it but I need to get more out of it and if that's not gonna happen then Idk
7/24/2021 6:35:12 AM	T XXX-XXX-8149	Dude on his way
7/24/2021 6:35:18 AM	MINOR 4 XXX-XXX-0341	k
7/30/2021 2:08:34 PM	MINOR 4 XXX-XXX-0341	Ok good, u should repost while you there so I can try and make sum incalls
7/30/2021 2:08:34 PM	MINOR 4 XXX-XXX-0341	So you can rest when you get back



7/30/2021 2:29:55 PM	T XXX-XXX-8149	Ok baby
7/30/2021 2:49:54 PM	MINOR 4 XXX-XXX-0341	Did you change the hour to 300? Bc on the bio it says you did

27. On August 8, 2021, DAVIS posted an ad for a commercial sex date with the title “THOR” under the number (XXX) XXX-1339 and on August 11, 2021, MINOR 3 posted for commercial sex dates utilizing the same phone number.

28. As part of this investigation, I conducted a search on Megapersonals and a law enforcement database that gathers commercial sex advertisements, and found advertisements depicting photographs of MINOR 1, MINOR 2, MINOR 3, and MINOR 4, advertising them for commercial sex in the Detroit area. The advertisements were posted on Megapersonals.eu, a website used to advertise commercial sex.

### **B. Training and Experience**

29. Based on my training, experience, and conversations with law enforcement agents who are experienced in the investigation of sex trafficking crimes, I am aware of the following:

- a. That people involved with sex trafficking utilize various online internet websites to advertise trafficking victims for the purposes of providing them to engage in commercial sex acts.
- b. That people involved with sex trafficking utilize email accounts to communicate with other traffickers, victims, and various websites to promote the illegal human trafficking activity.
- c. That people involved with sex trafficking utilize cellular telephones to communicate either via text messaging, photo messaging, email or voice calling to facilitate the criminal activity. Cellular telephones are often used for communication between the victims of human trafficking and the traffickers and the purchasers of commercial sexual acts. Additionally, cellular telephones are used as the primary device to produce images and post online advertisements for commercial sexual activity.
- d. That people involved in criminal activity such as sex trafficking often use multiple cellular phones to conceal their criminal activity.
- e. That cellular devices, as part of the initial setup of the device, request the establishment of a cloud-based account to back up information for

the purpose of recovering lost data, and enables users to recover the data to a separate device.

30. The SUBJECT DEVICE is currently in the lawful possession of the FBI. It came into the FBI's possession, when seized incident to the arrest of DAVIS, as described above. Therefore, while the FBI might already have all necessary authority to examine the SUBJECT DEVICE, I seek this additional warrant out of an abundance of caution to be certain that an examination of the SUBJECT DEVICE will comply with the Fourth Amendment and other applicable laws.

31. The SUBJECT DEVICE is currently in storage at the FBI's Detroit Field Office Evidence Control Room, 477 Michigan Ave, Detroit, MI 48226. In my training and experience, I know that the SUBJECT DEVICE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were with the SUBJECT DEVICE first came into the possession of the FBI.

32. The FBI believes information stored in the SUBJECT DEVICE will reveal evidence related to violations of 18 U.S.C. § 1591 (Sex Trafficking of Children or by Force, Fraud or Coercion) by DAVIS.

### **TECHNICAL TERMS**

33. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless

telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data.

Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet

traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

34. Based on my training, experience, and research, I know that the SUBJECT DEVICE has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

35. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things



that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

36. As described above and in Attachment B, this application seeks permission to search for evidence of violations of 18 U.S.C. § 1591 that might be found on the SUBJECT DEVICE, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

37. *Probable cause.* I submit that there is probable cause to believe evidence of violations of the Specified Federal Offenses will be stored on the target's cellular phone (the SUBJECT DEVICE), for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a

computer or cellular phone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer or cellular phone’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, cellular phones contain electronic evidence of how the phones have been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Cell phone users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or “cache.”

38. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how cellular phones were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT DEVICE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of other external

storage media, and the times the computer was in use. File systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a cellular phone and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element, or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a cellular phone or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatng or

exculpating the cell phone owner. Further, cell phone and storage media activity can indicate how and when the cell phone or storage media was accessed or used. For example, as described herein, cell phones typically contain information that log: cell phone user account session times and durations, cell phone activity, electronic storage media that connected with the cell phone, and the IP addresses through which the cell phone accessed networks and the internet. Such information allows investigators to understand the chronological context of cell phone or electronic storage media access, use, and events relating to the crime under investigation. Additionally, information stored within a cell phone can provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a cell phone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media. The geographic and timeline information described herein may either inculcate or

exculpate the cell phone user. Last, information stored within a cell phone may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information within the cell phone may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the cell phone or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, cell phone evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a cell phone is evidence may depend on other information stored on the phone and the application of knowledge about how a cell phone behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a cell phone was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

39. I know that when an individual uses a cell phone to facilitate sex trafficking, the individual's cell phone will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The phone is an instrumentality of the crime because it is used as a means of committing the criminal offense (for example, the cell phone is used to access the internet to post commercial sex advertisements or to communicate with or recruit victims). The phone is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a cell phone used to commit a crime of this type may contain: internet browsing history relating to commercial sex advertisements, text messages and social media messages with victims, photographs used to post advertisements, data that is evidence of how the cell phone was used; data that was sent or received; notes as

to how the criminal conduct was achieved; records of internet discussions about the crime; and other records that indicate the nature of the offense.

40. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

41. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

### **CONCLUSION**

42. Based on the above factual information, I respectfully submit that there is probable cause to believe that evidence and instrumentalities of violations of 18 U.S.C. § 1591 (Sex Trafficking of Children or by Force, Fraud or Coercion) may be found on the SUBJECT DEVICE.




43. Therefore, I request a search warrant authorizing a search of the item in Attachment A for the items described in Attachment B.


**REQUEST FOR SEALING**

44. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

  
\_\_\_\_\_  
Michael Strunk  
Task Force Officer  
Federal Bureau of Investigation

Sworn to before me and signed in my  
presence and/or by reliable electronic means

  
\_\_\_\_\_  
Hon. Patricia T. Morris  
United States Magistrate Judge

Dated: August 20, 2021

**ATTACHMENT A**  
**Property to Be Searched**

The device to be searched is the following cellular phone seized from  
TORIANO CORNELL DAVIS on August 11, 2021:

(1) silver Apple iPhone 12 Pro Max (the SUBJECT DEVICE).

The SUBJECT DEVICE is located at the FBI's Detroit Field Office Evidence  
Control Room, 477 Michigan Ave, Detroit, MI 48226. This warrant authorizes the  
forensic examination of the SUBJECT DEVICE for the purpose of identifying the  
electronically stored information described in Attachment B.

**ATTACHMENT B**  
**Particular Things to Be Seized**

1. All records on the SUBJECT DEVICE described in Attachment A that relate to violations of 18 U.S.C. § 1591 (Sex Trafficking of Children or by Force, Fraud or Coercion) and involve TORIANO CORNELL DAVIS, including:

- a. Content of all call logs, contact lists, text messages, iMessages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, voicemails, social media account activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits, or instrumentalities of the violation described above;
- b. Evidence of location services information within the phone;
- c. Evidence of the times the SUBJECT DEVICE was used;
- d. Passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT DEVICE;
- e. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violation described below, and any and all

other data contained therein, in relation to the violations of 18 U.S.C. § 1591 (Sex Trafficking of Children or by Force, Fraud or Coercion).

2. Evidence of user attribution showing who used or owned the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy

of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Hon. Patricia T. Morris      U. S. Magistrate Judge  
\_\_\_\_\_  
*Printed name and title*

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*